## 21IT1504 - EMBEDDED SYSTEMS AND INTERNET OF THINGS

## UNIT- III INTRODUCTION TO IOT

Internet of Things - Physical and Logical Design- IoT Enabling Technologies - IoT Levels & Deployment Templates – Four Pillars of IoT-M2M-RFID-WSN-SCAD

**Internet of Things:** A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities, use intelligent interfaces, are seamlessly integrated into the information network, and often communicate data associated with users and their environments

### Characteristics:

Dynamic and Self-Adapting:- IoT devices and system may have the capability to change dynamically depending upon the system and operating conditions or sensed environment. For example, the surveillance cameras can change their modes based on day or night.

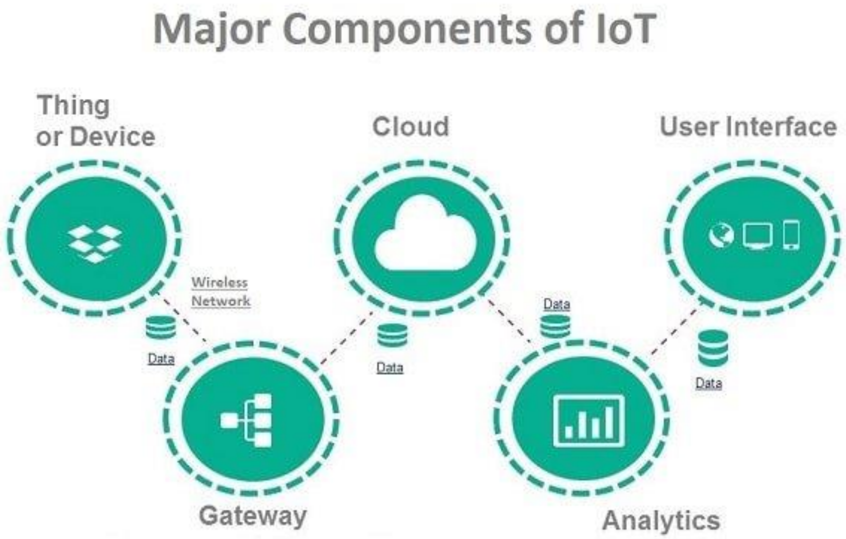
Self-configuring:- IoT devices have self-configuring capability which allows large number of devices to work together to work provide certain functionality they can change their networking and update the software automatically.

Interoperable Communication Protocol: - IoT devices can communicate with number of interoperable (communicate with other devices without special effort) communication protocols.

Unique ID: - IoT devices have a unique identity differentiated with unique IP address.

Integrated into Information Network: - IoT devices are integrated into the information network that allows them to communicate and exchange data with other devices and system.

### COMPONENTS of IoT:



IoT is a transformation process of connecting our smart devices and objects to a network to perform efficiently and access remotely.

## 1. Smart devices and sensors – Device connectivity

Devices and sensors are the components of the device connectivity layer. These smart sensors are continuously collecting data from the environment and transmit the information to the next layer.

The latest techniques in semiconductor technology are capable of producing micro smart sensors for various applications.

Common sensors are:

- Temperature sensors and thermostats
- Pressure sensors
- Humidity / Moisture level
- Light intensity detectors
- Moisture sensors
- Proximity detection
- RFID tags

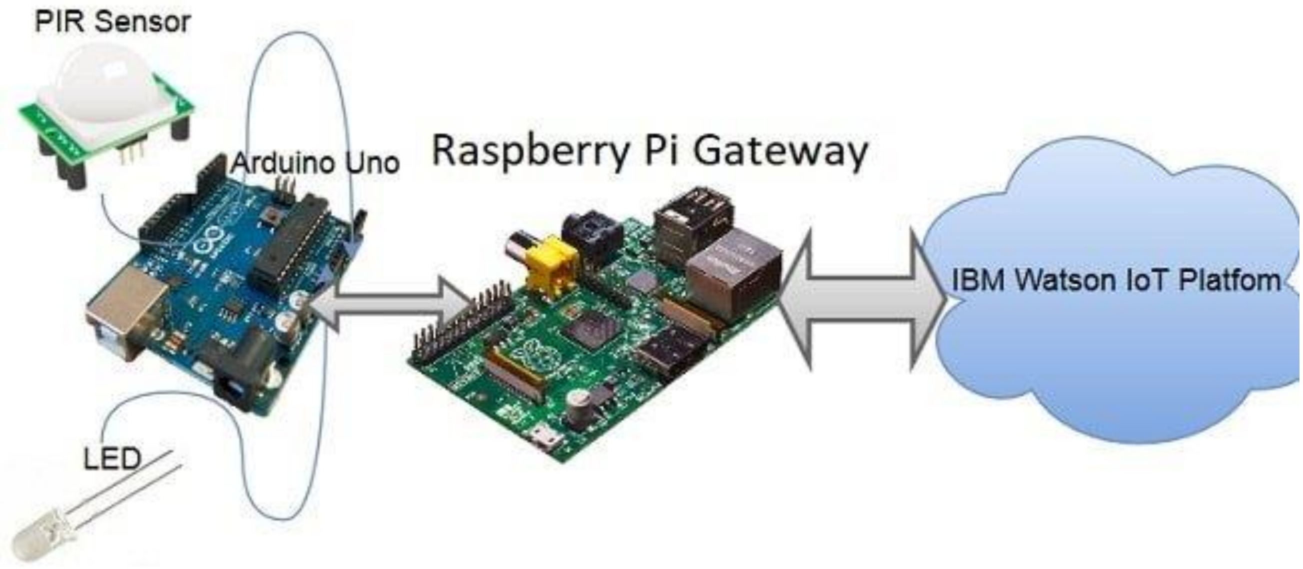
### How are the devices connected?

Most modern smart devices and sensors can be connected to low-power wireless networks like Wi-Fi, ZigBee, Bluetooth, Z-wave, LoRAWAN, etc. Each of these wireless technologies has its pros and cons in terms of power, data transfer rate, and overall efficiency.

Developments in low-power, low-cost wireless transmitting devices are promising in the area of IoT due to their long battery life and efficiency. Many companies have adopted the latest protocols like 6LoWPAN- IPv6 over Low Power Wireless Personal Area Networks to implement energy-efficient data transmission for IoT networks.

6LoWPAN uses reduced transmission time (typically short time pulses) and thus saves energy.

## 2. Gateway



IoT Gateway manages the bidirectional data traffic between different networks and protocols. Another function of the gateway is to translate different network protocols and make sure interoperability of the connected devices and sensors.

Gateways can be configured to perform pre-processing of the collected data from thousands of sensors locally before transmitting it to the next stage. In some scenarios, it would be necessary due to the compatibility of the TCP/IP protocol.

IoT gateway offers a certain level of security for the network and transmitted data with higher-order encryption techniques. It acts as a middle layer between devices and the cloud to protect the system from malicious attacks and unauthorized access.

## 3. Cloud

The Internet of Things creates massive data from devices, applications, and users, which has to be managed in an efficient way. IoT cloud offers tools to collect, process, manage and store huge amounts of data in real time. Industries and services can easily access these data remotely and make critical decisions when necessary.
Basically, the IoT cloud is a sophisticated, high-performance network of servers optimized to perform high-speed data processing of billions of devices, traffic management, and deliver accurate analytics. Distributed database management systems are one of the most important components of the IoT cloud.

Cloud system integrates billions of devices, sensors, gateways, protocols, and data storage and provides predictive analytics. Companies use these analytics data to improve products and services, preventive measures for certain steps, and build their new business model accurately.

### 4. Analytics

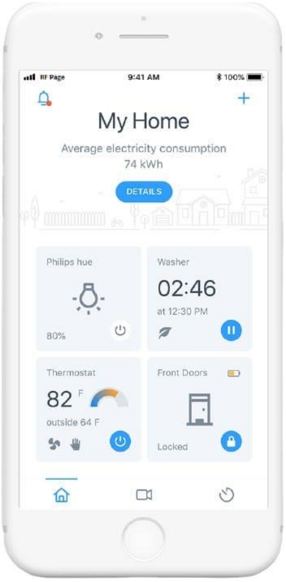
Analytics is the process of converting analog data from billions of smart devices and sensors into useful insights which can be interpreted and used for detailed analysis. Smart analytics solutions are inevitable for IoT systems for the management and improvement of the entire system.

One of the major advantages of an efficient IoT system is real-time smart analytics which helps engineers to find out irregularities in the collected data and act fast to prevent an undesired scenario.  Service providers can prepare for further steps if the information is collected accurately at the right time.

Big enterprises use the massive data collected from IoT devices and utilize the insights for their future business opportunities. Careful analysis will help organizations to predict trends in the market and plan ahead for a successful implementation.

Information is very significant in any business model, and predictive analysis ensures success in the concerned area of the business line.

### 5. User interface



User interfaces are the visible, tangible part of the IoT system which users can access. It is one of the significant components of Internet of things where user control the system and collect information. Designers will have to make sure of a well-designed user interface for minimum effort for users and encourage more interactions. Modern technology offers much interactive design to ease complex tasks into simple touch panel controls. Multicolor touch panels have replaced hard switches in our household appliances, and the trend is increasing for almost every smart home device.

The user interface design has higher significance in today’s competitive market; it often determines the user whether to choose a particular device or appliance. Users will be interested in buying new devices or smart gadgets if it is very user-friendly and compatible with common wireless standards.

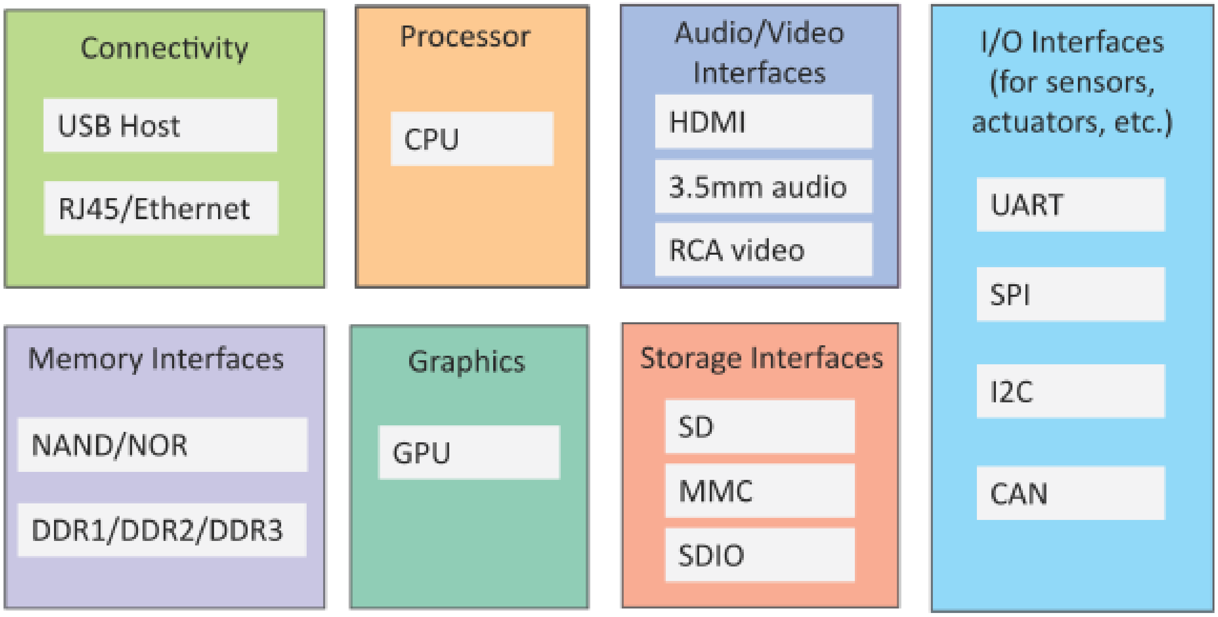
## PHYSICAL DESIGN OF IoT

### 1.Things in IoT

- The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing and actuating and have monitoring capabilities.
- IoT devices can:
  - Exchange data with other connected devices and applications (directly or indirectly), or
  - Collect data from other devices and process the data locally, or
  - Send the data to centralized servers or cloud-based application back-ends for processing the data, or
  - Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints

### Generic Block Diagram of an IoT Device

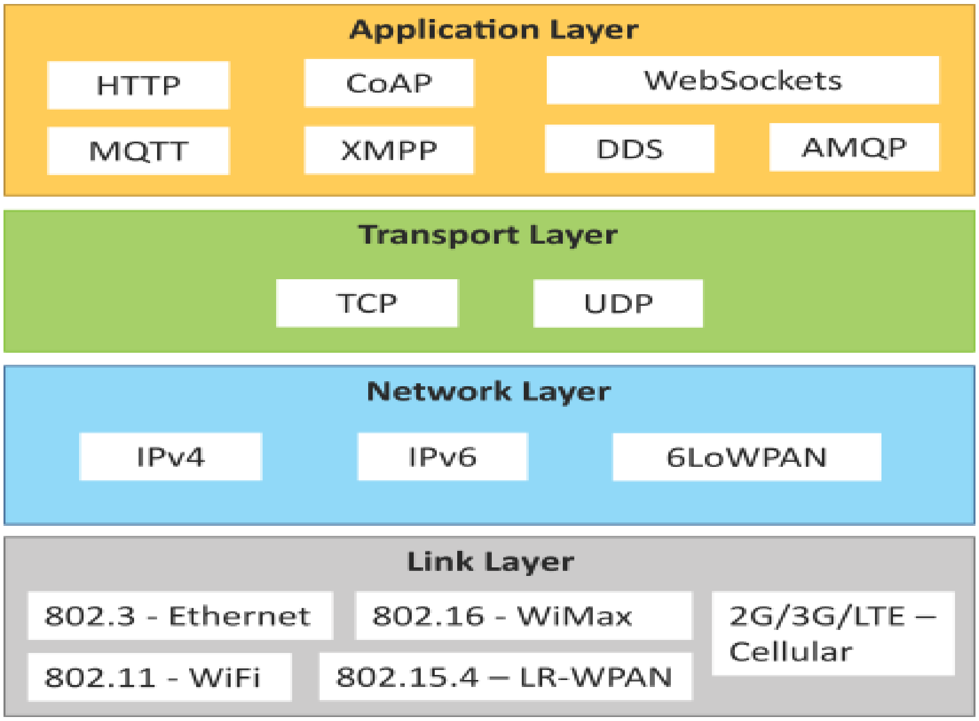
- An IoT device may consist of several interfaces for connections to other devices, both wired and wireless.
  - I/O interfaces for sensors
  - Interfaces for internet connectivity
  - Memory and storage interfaces
  - Audio/video interfaces



**2.IoT Protocols**

- Link Layer
  - 802.3 – Ethernet
  - 802.11 – WiFi
  - 802.16 – WiMax
  - 802.15.4 – LR-WPAN
  - 2G/3G/4G
- Network/Internet Layer
  - IPv4
  - IPv6
  - 6LoWPAN
- Transport Layer
  - TCP
  - UDP
- Application Layer
  - HTTP
  - CoAP

- WebSocket
- MQTT
- XMPP
- DDS
- AMQP



**Link Layer**

This protocol determines how the data is physically sent over the network layer (e.g. copper wire, coaxial cable or a radio wave). It determines how the packet are coded and signaled by the hardware device over the medium to which the host is attached.

802.3-Ethernet:

•IEEE802.3 is collection of wired Ethernet standards for the link layer. Eg: 802.3 uses co-axial cable; 802.3i uses copper twisted pair connection; 802.3j uses fiber optic connection; 802.3ae uses Ethernet overfiber.

• 802.11-WiFi: IEEE802.11 is a collection of wireless LAN(WLAN) communication standards including extensive description of link layer. Eg: 802.11a operates in 5GHz band, 802.11b and 802.11g operates in 2.4GHz band, 802.11n operates in 2.4/5GHz band, 802.11ac operates in 5GHz band, 802.11ad operates in 60Ghzband.

• 802.16 - WiMax: IEEE802.16 is a collection of wireless broadband standards including exclusive description of link layer. WiMax provide data rates from 1.5 Mb/s to 1Gb/s.

• 802.15.4-LR-WPAN: IEEE802.15.4 is a collection of standards for low rate wireless personal area network(LR-WPAN). Basis for high level communication protocols such as ZigBee. Provides data rate from 40kb/s to250kb/s.

•2G/3G/4G-Mobile Communication: Data rates from 9.6kb/s(2G) to up to100Mb/s(4G).

**Network/Internet Layer**

The network layers are responsible for sending of IP datagram's from the source network to the destination network. It performs host addressing and packet routing. The datagram's consists of source and destination addresses where host identifies using IP schemes as IPV4 and IPV6.

- ➢ IPV4:- It is used to identify the devices on a network using hierarchical addressing scheme. It uses 32- bit address that allows total 2^32 or 4 billion devices 128
- ➢ IPV6:- It is the new version of internet protocol which uses 128-bits address that allows 2^128 or 3 X 10^38 address.

• Transport Layer The transport layer protocols provide end to end message transfer capability independent of the underlying network. The function of the transport layer is to provide functions such as error control, segmentation, floe control and congestion control.

- ➢ TCP: - It is most widely used for data transmission in communication network such as internet .it provides process to process communication using port numbers. It uses port number for communication which keeps Track of segments that are received and transmitted.
- ➢ UDP: - It is the simplest protocol that involves minimum amount of communication mechanism. It is connectionless, unreliable transport protocol. It does not provide guaranteed delivery of the message.

**Application Layer:**

Defines how the applications interface with lower layer protocols to send data over the n/w. Enables process-to-process communication using ports.

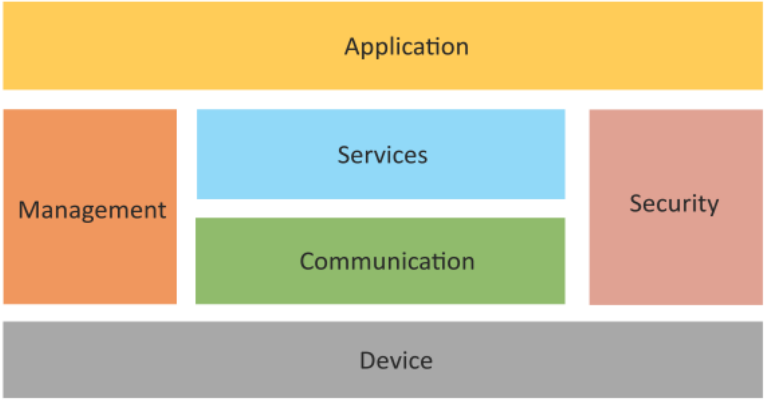
Protocols:

- ➢ HTTP: Hyper Text Transfer Protocol that forms foundation of WWW. Follow requestresponse model Stateless protocol.
- ➢ CoAP: Constrained Application Protocol for machine-to-machine(M2M) applications with constrained devices, constrained environment and constrained n/w. Uses clientserver architecture.
- ➢ Web Socket: allows full duplex communication over a single socket connection.
- ➢ MQTT: Message Queue Telemetry Transport is light weight messaging protocol based on publish-subscribe model. Uses client server architecture. Well suited for constrained environment.
- ➢ XMPP: Extensible Message and Presence Protocol for real time communication and streaming XML data between network entities. Support client-server and server-server communication.

- DDS: Data Distribution Service is data centric middleware standards for device-to-device or machine-to-machine communication. Uses publish-subscribe model.
- AMQP: Advanced Message Queuing Protocol is open application layer protocol for business messaging. Supports both point-to-point and publish-subscribe model.

## LOGICAL DESIGN OF IOT

- Logical design of an IoT system refers to an abstract representation of the entities and processes without going into the low-level specifics of the implementation.
- An IoT system comprises a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication and management.



- Device: An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions. • Communication: handles the communication for IoT system.
- Services: for device monitoring, device control services, data publishing services and services for device discovery.
- Management: Provides various functions to govern the IoT system.
- Security: Secures IoT system and priority functions such as authentication, authorization, message and context integrity and data security.
- Application: IoT application provide an interface that the users can use to control and monitor various aspects of IoT system.

**IoT Communication Models:**

1) Request-Response

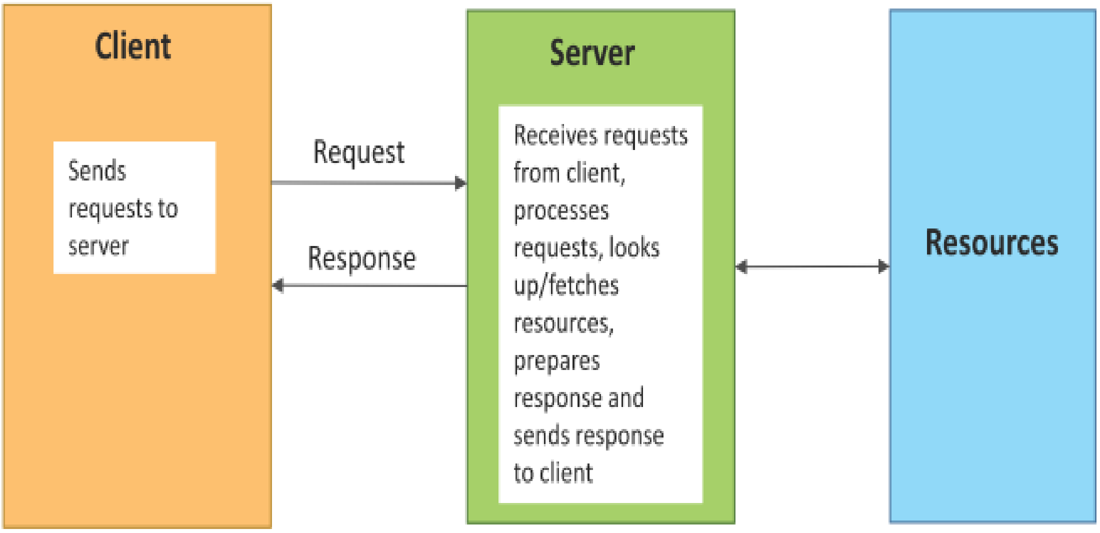
2) Publish-Subscibe

3)Push-Pull

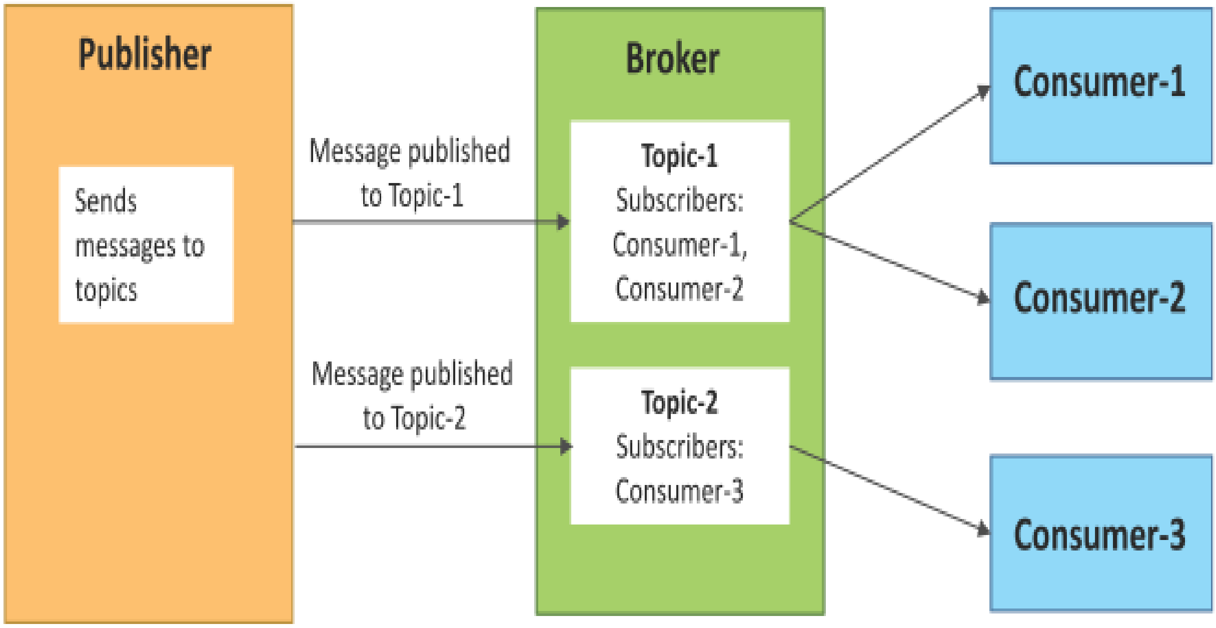
4) Exclusive Pair

### Request–Response Communication Model

- Request–Response is a communication model in which the client sends requests to the server and the server responds to the requests.
- When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response and then sends the response to the client.

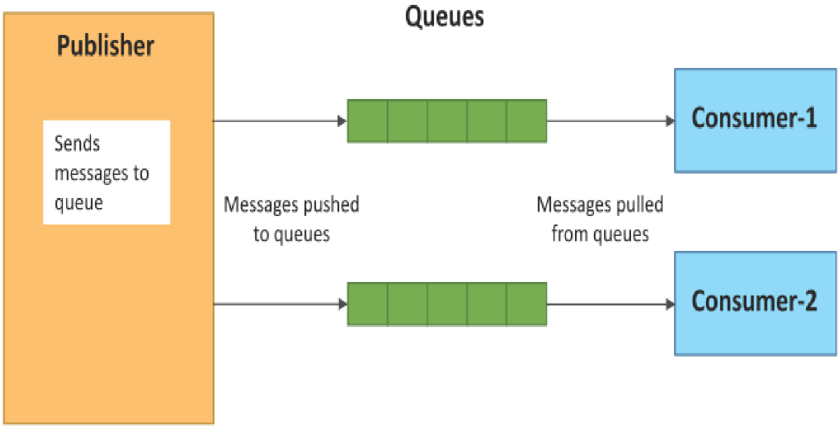

Client
Sends requests to server
Request
Response
Server
Receives requests from client, processes requests, looks up/fetches resources, prepares response and sends response to client
Resources

### Publish–Subscribe Communication Model



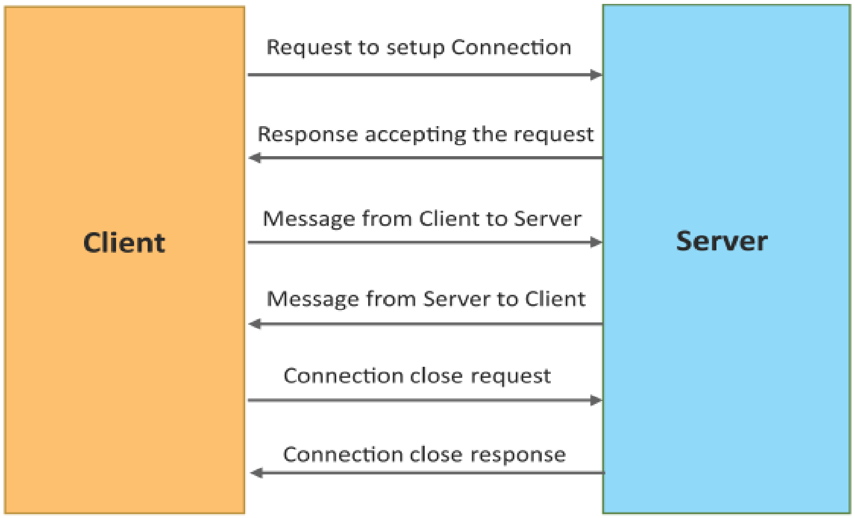
### Push–Pull Communication Model

- Push–Pull is a communication model in which the data producers push the data to queues and the consumers pull the data from the queues. Producers do not need to be aware of the consumers.
- Queues help in decoupling the messaging between the producers and consumers.
- Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which the consumers pull data.



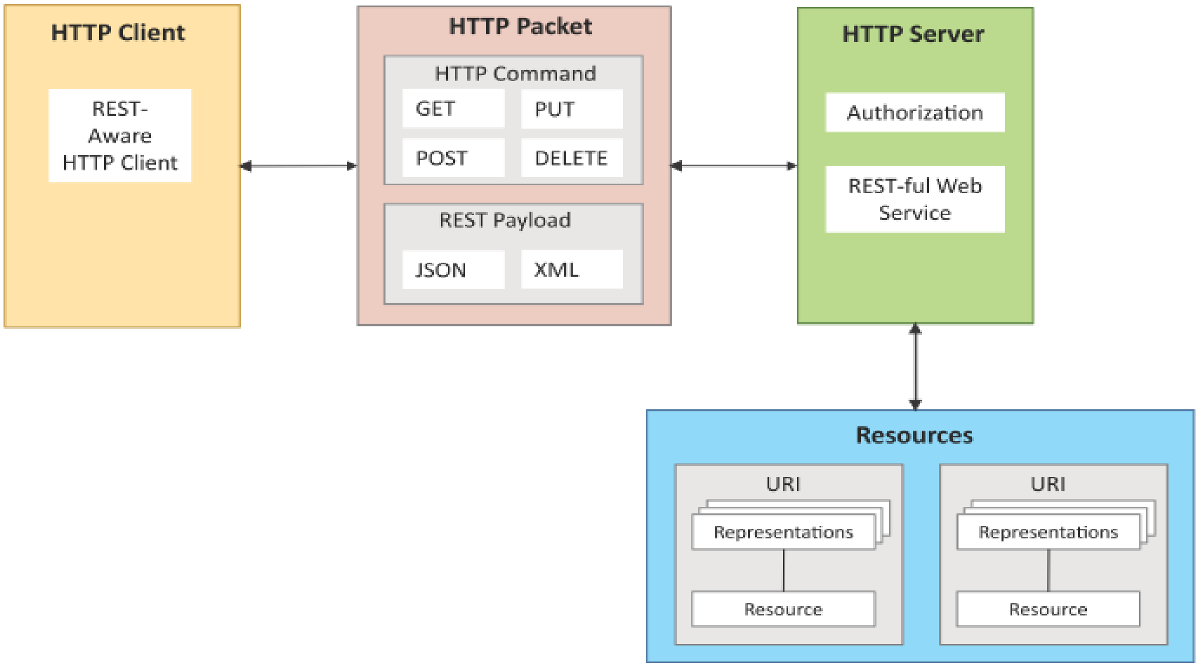
### Exclusive Pair Communication Model

- Exclusive Pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and the server.
- Once the connection is set up it, remains open until the client sends a request to close the connection.
- Client and server can send messages to each other after connection setup.


Request to setup Connection
Response accepting the request
Client
Message from Client to Server
Server
Message from Server to Client
Connection close request
Connection close response

## REST-based Communication APIs

- Representational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred.
- REST APIs follow the request–response communication model.
- REST architectural constraints apply to the components, connectors and data elements within a distributed hypermedia system.



Client-server – The principle behind the client-server constraint is the separation of concerns. for example clients should not be concerned with the storage of data which is concern of the serve. Similarly the server should not be concerned about the user interface, which is concern of the clien. Separation allows client and server to be independently developed and updated.

Stateless – Each request from client to server must contain all the information necessary to understand the request, and cannot take advantage of any stored context on the server. The session state is kept entirely on the client.

Cache-able – Cache constraints requires that the data within a response to a request be implicitly or explicitly leveled as cache-able or non cache-able. If a response is cache-able, then a client cache is given the right to reuse that repsonse data for later, equivalent requests. caching can partially or completely eliminate some instructions and improve efficiency and scalability.

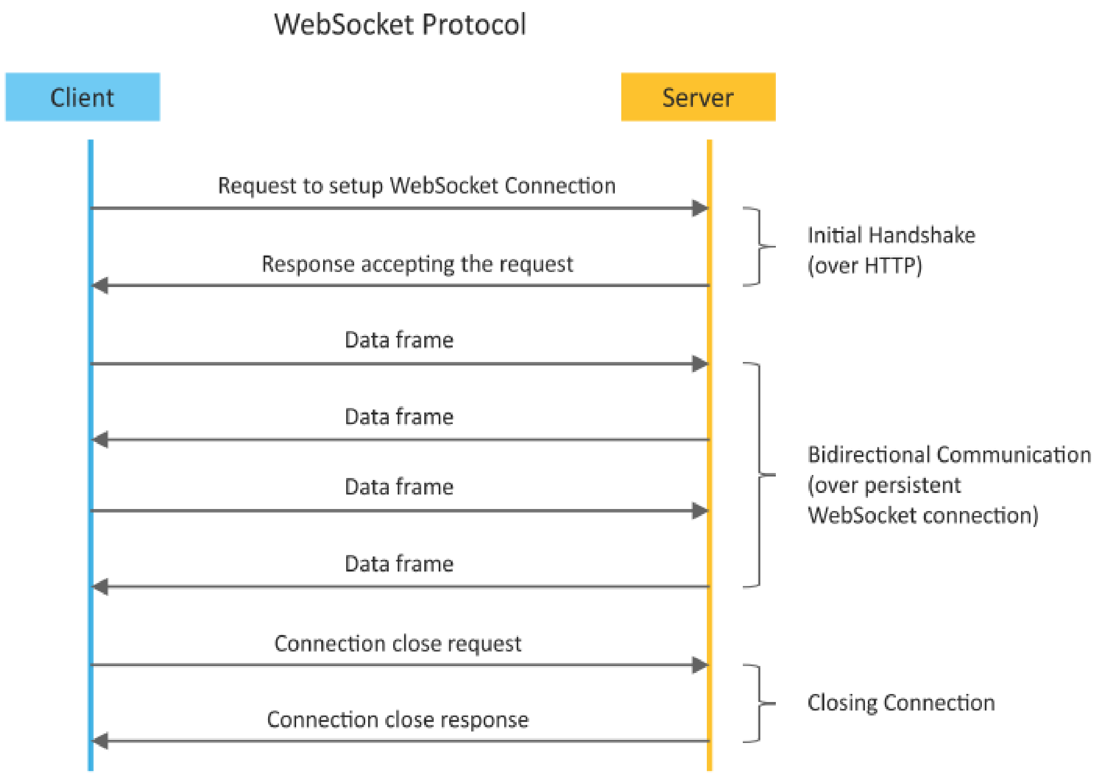
Layered system – layered system constraints, constrains the behavior of components such that each component cannot see beyond the immediate layer with they are interacting. For example, the client cannot tell whether it is connected directly to the end server or two an intermediary along the way. System scalability can be improved by allowing intermediaries to respond to requests instead of the end server, without the client having to do anything different.

Uniform interface – uniform interface constraints requires that the method of communication between client and server must be uniform. Resources are identified in the requests (by URIs in web based systems) and are themselves is separate from the representations of the resources data returned to the client. When a client holds a representation of resources it has all the information required to update or delete the resource you (provided the client has required permissions). Each message includes enough information to describe how to process the message.

Code on demand – Servers can provide executable code or scripts for clients to execute in their context. this constraint is the only one that is optional. A RESTful web service is a " Web API " implemented using HTTP and REST principles. REST is most popular IoT Communication APIs

**Web Socket-based Communication APIs**

- Web Socket APIs allow bi-directional, full duplex communication between clients and servers.
- Web Socket APIs follow the exclusive pair communication model.
- Unlike request-response model such as REST, the Web Socket APIs allow full duplex communication and do not require new connection to be setup for each message to be sent.
- Web socket communication begins with a connection setup request sent by the client to the server.
- The request (called web socket handshake) is sent over HTTP and the server interprets it is an upgrade request. If the server supports web socket protocol, the server responds to the web socket handshake response.
- After the connection setup client and server can send data/messages to each other in full duplex mode. Web socket
- API reduce the network traffic and latency as there is no overhead for connection setup and termination requests for each message.
- Web socket suitable for IoT applications that have low latency or high throughput requirements. So Web socket is most suitable IoT Communication APIs for IoT System.


WebSocket Protocol
Client
Server
Request to setup WebSocket Connection
Response accepting the request
Initial Handshake (over HTTP)
Data frame
Data frame
Data frame
Data frame
Bidirectional Communication (over persistent WebSocket connection)
Connection close request
Connection close response
Closing Connection

## IoT(internet of things) enabling technologies

IoT (internet of things) enabling technologies are
1. Wireless Sensor Network
2. Cloud Computing
3. Big Data Analytics
4. Communications Protocols
5. Embedded System

### 1. Wireless Sensor Network(WSN) :

A WSN comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A wireless sensor network consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.

Example –

- Weather monitoring system
- Indoor air quality monitoring system
- Soil moisture monitoring system
- Surveillance system
- Health monitoring system

### 2. Cloud Computing :

It provides us the means by which we can access applications as utilities over the internet.

Cloud means something which is present in remote locations.
With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.
**Characteristics –**

1. Broad network access
2. On demand self-services
3. Rapid scalability
4. Measured service
5. Pay-per-use

Provides different services, such as –

- **IaaS (**Infrastructure as a service**)**
  Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.
  Ex : Web Hosting, Virtual Machine etc.
- **PaaS (**Platform as a service**)**
  Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it provides a platform to develop applications.
  Ex : App Cloud, Google app engine
- **SaaS (**Software as a service**)**
  It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.
  SaaS Applications are sometimes called web-based software on demand software or hosted software.
  SaaS applications run on a SaaS provider’s service and they manage security availability and performance.
  Ex : Google Docs, Gmail, office etc.

**3. Big Data Analytics :**
It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.
Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.
Several steps involved in analyzing big data –

1. Data cleaning
2. Munging
3. Processing
4. Visualization

Examples –

- Bank transactions
- Data generated by IoT systems for location and tracking of vehicles
- E-commerce and in Big-Basket
- Health and fitness data generated by IoT system such as a fitness bands

**4. Communications Protocols :**

They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.

They are used in

1. Data encoding
2. Addressing schemes

**5. Embedded Systems :**

It is a combination of hardware and software used to perform special tasks.

It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc. ) and storage devices (flash memory).

It collects the data and sends it to the internet.

Embedded systems used in

Examples –

1. Digital camera
2. DVD player, music player
3. Industrial robots
4. Wireless Routers etc.

## IoT Levels and Deployment Templates

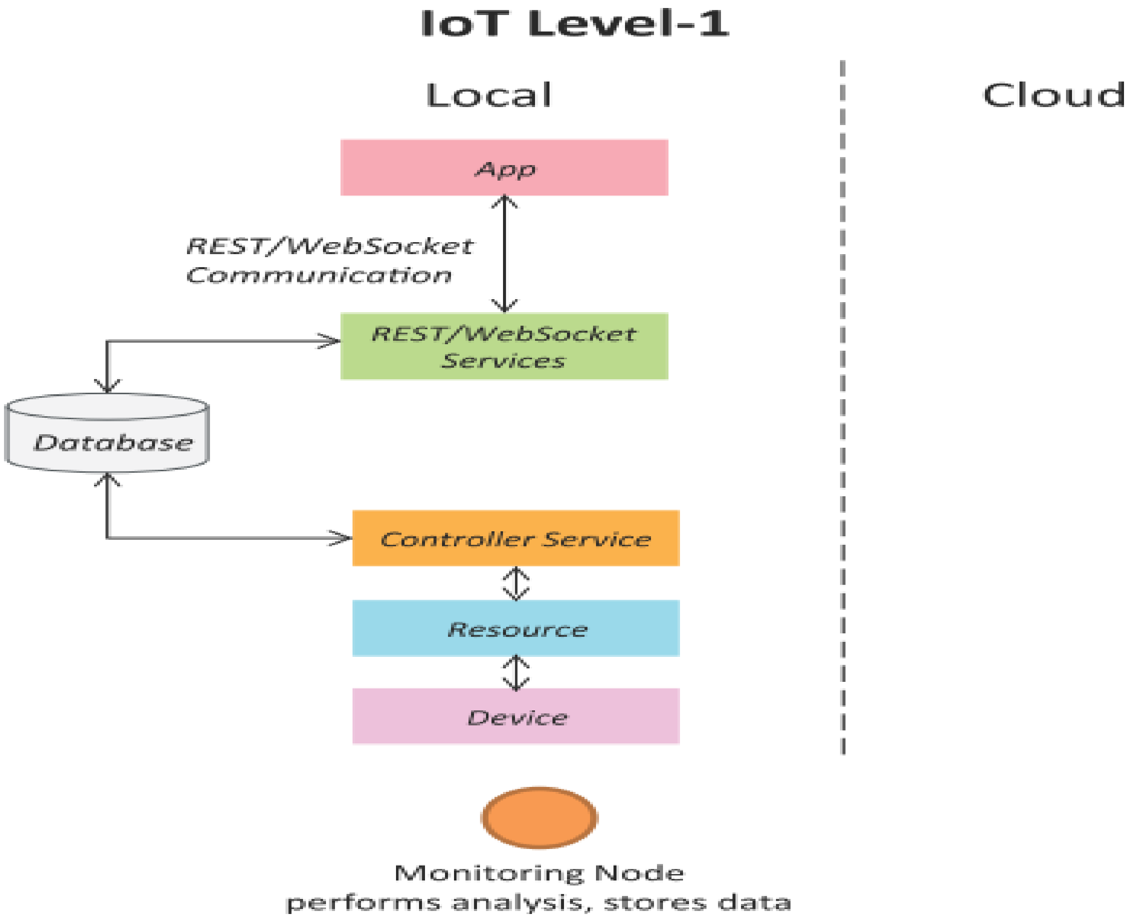
An IoT system comprises the following components:

- **Device**: An IoT device allows identification, remote sensing, actuating and remote monitoring capabilities.
- **Resource**: Resources are software components on the IoT device for accessing, processing and storing sensor information, or for controlling actuators connected to the device. Resources also include the software components that enable network access for the device.
- **Controller Service**: Controller service is a native service that runs on the device and interacts with the web services. Controller service sends data from the device to the web service and receives commands from the application (via web services) for controlling the device.
- **Database**: Database can be either local or in the cloud and stores the data generated by the IoT device.

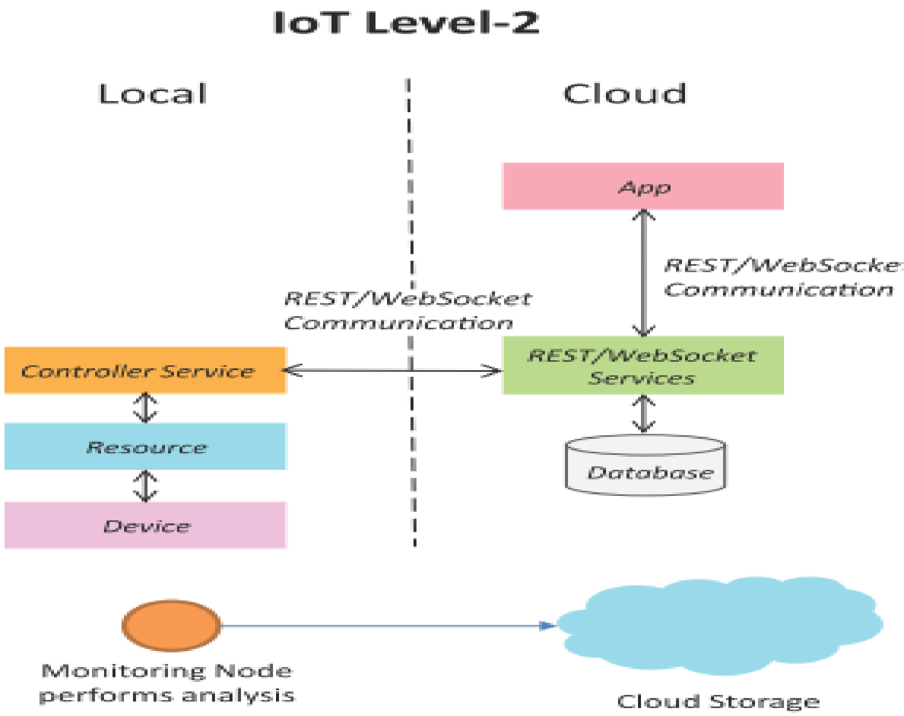
- **Web Service**:  Web services serve as a link between the IoT device, application, database and analysis components.  Web service can be implemented using HTTP and REST principles (REST service) or using the WebSocket protocol (WebSocket service).
- **Analysis Component**: This is responsible for analyzing the IoT data and generating results in a form that is easy for the user to understand.
- **Application**: IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and the processed data.

**IoT Level-1**

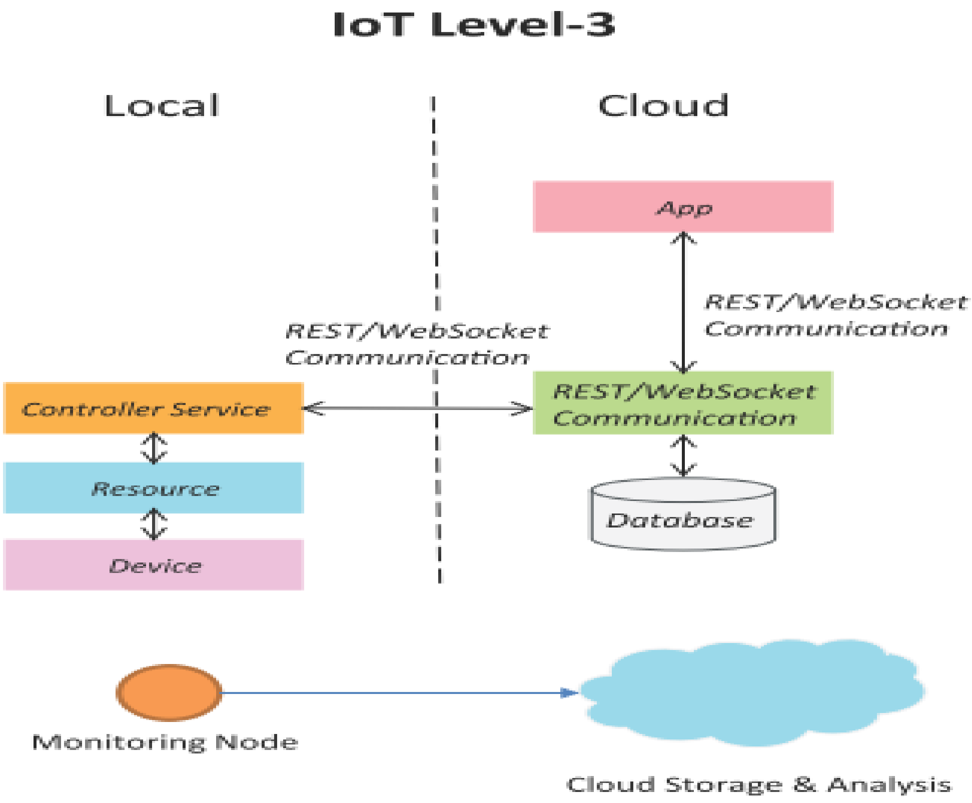
- A level-1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application.
- Level-1 IoT systems are suitable for modelling low-cost and low-complexity solutions where the data involved is not big and the analysis requirements are not computationally intensive



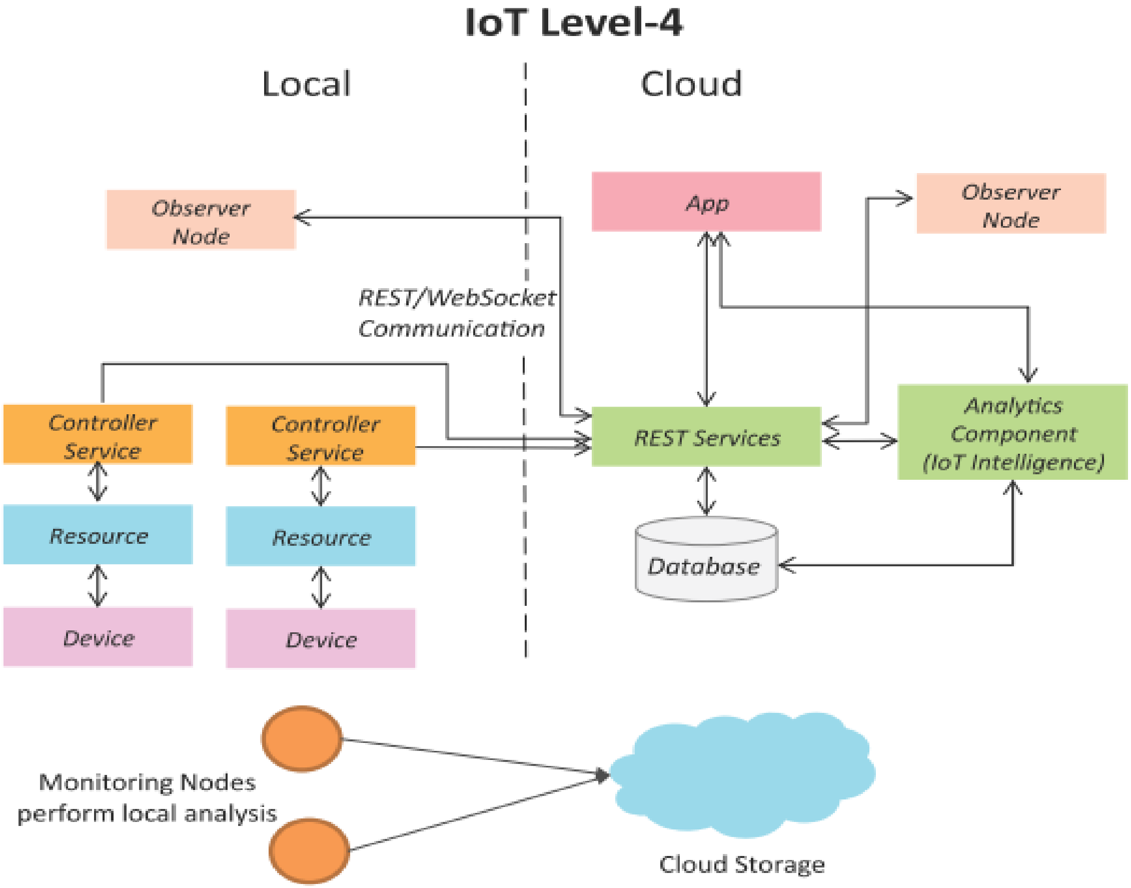
## IoT Level-2



## IoT Level-3



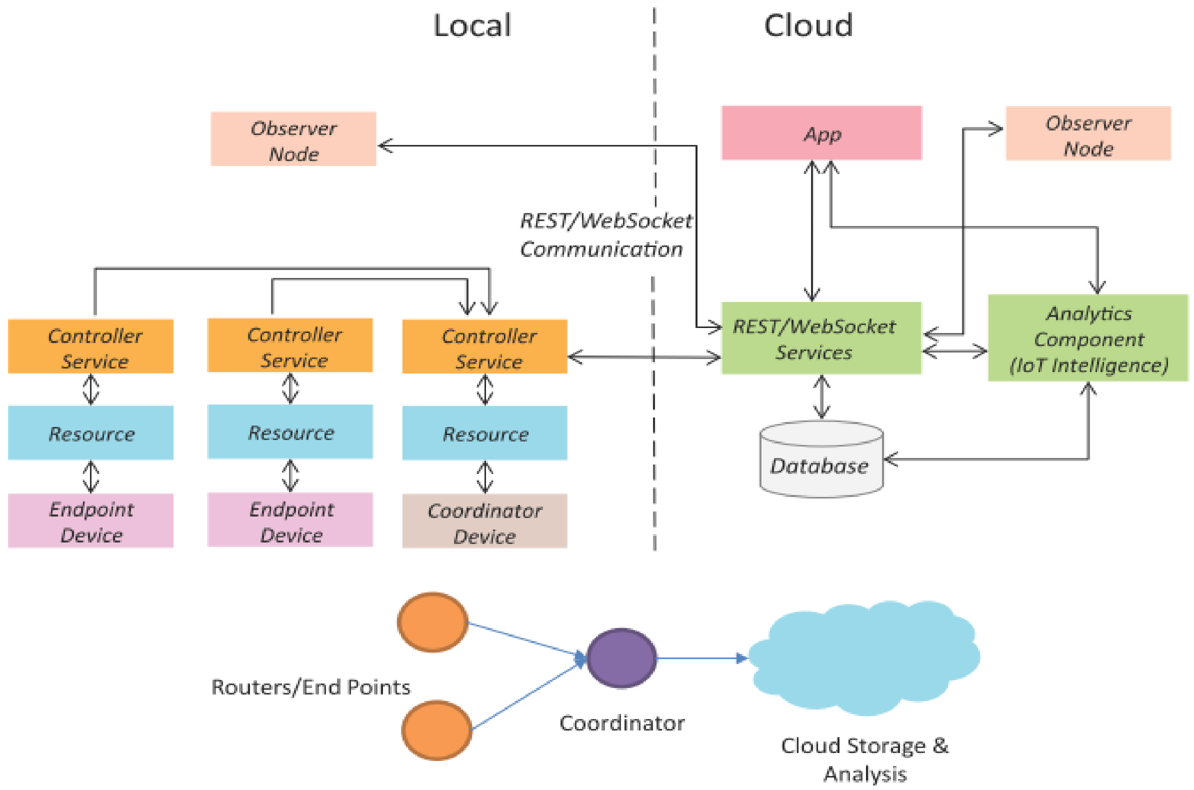
**IoT Level-4**



**IoT Level-5**

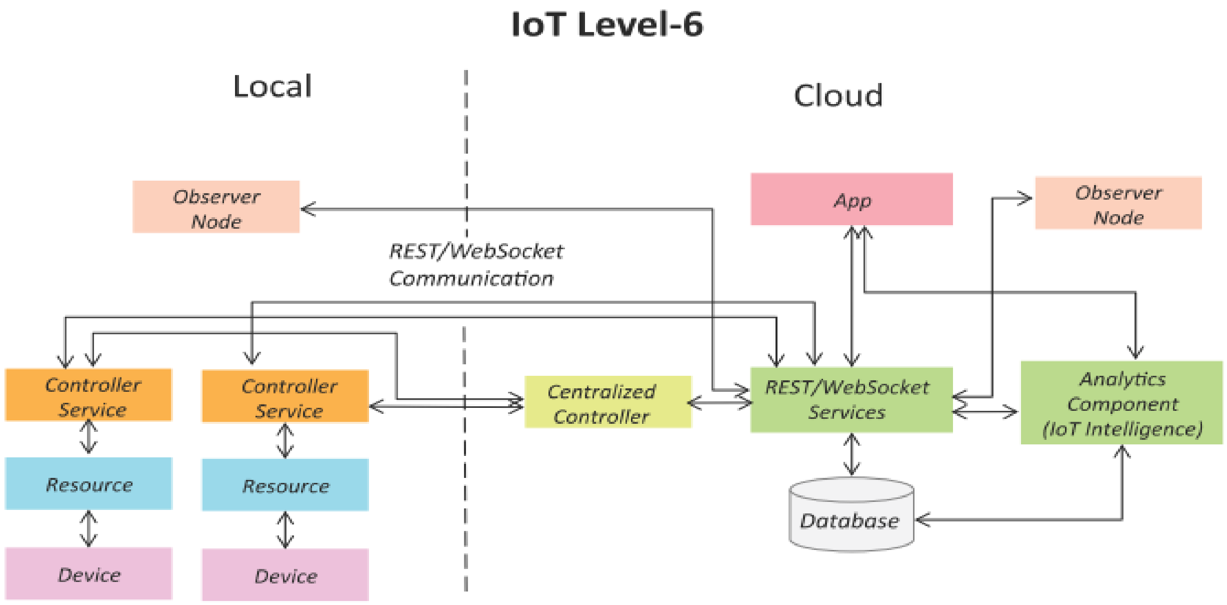
- A level-5 IoT system has multiple end nodes and one coordinator node.
- The end nodes perform sensing and/or actuation.
- The coordinator node collects data from the end nodes and sends it to the cloud.
- Data is stored and analyzed in the cloud and the application is cloud-based.
- Level-5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.

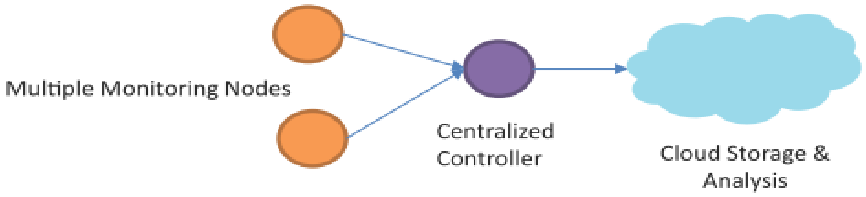
## IoT Level-5



### IoT Level-6

- A level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud.
- Data is stored in the cloud and the application is cloud-based.
- The analytics component analyzes the data and stores the results in the cloud database.
- The results are visualized with the cloud-based application.
- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes





**Domain Specific IoTs**

IoT Applications for :

- Home
- Cities
- Environment
- Energy Systems
- Retail
- Logistics
- Industry
- Agriculture
- Health & Lifestyle

**Smart Home :**

- Smart parking
- Smart lighting
- Smart Appliances
- Intrusion Detection
- Smoke / Gas Detectors

### Smart parking

- Sensors are used for each parking slot, to detect whether the slot is occupied or not.
- This information is aggregated by local controllers and sent over the Internet to the database.
- Drivers can use an application to know about empty parking slots.

### Smart Lighting

- Smart lighting achieves energy savings by sensing the human movements and their environments and controlling the lights accordingly.
- Key enabling technologies for smart lighting include : - Solid state lighting (such as LED lights) - IP-enabled lights
- Wireless-enabled and Internet connected lights can be controlled remotely from IoT applications such as a mobile or web application.

### Smart Appliances

Smart appliances make the management easier and provide status information of appliances to the users remotely.

E.g: smart washer/dryer that can be controlled remotely and notify when the washing/drying cycle is complete.

- Open Remote is an open source automation platform for smart home and building that can control various appliances using mobile and web applications.
- It comprises of three components: -
    - ➢ Controller-> manages scheduling and runtime integration between devices.
    - ➢ Designer -> allows to create both configuration for the controller and user interface designs
    - ➢ Control Panel -> allows to interact with devices and control them.

### Intrusion Detection

- Home intrusion detection systems use security cameras and sensors to detect intrusions and raise alerts.
- The form of the alerts can be in form: - SMS - Email - Image grab or a short video clip as an email attachment

### Smoke / Gas Detectors

- Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire.
- It uses optical detection, ionization or air sampling techniques to detect smoke
- The form of the alert can be in form : Signals that send to a fire alarm system
- Gas detector can detect the presence of harmful gases such as carbon monoxide (CO), liquid petroleum gas (LPG), etc.

**Smart Cities**

1. Smart Parking
2. Smart Lighting for Road
3. Smart Road
4. Structural Health Monitoring
5. Surveillance

- Emergency Response

**2.Smart Lighting for Roads**

• It can help in saving energy

• Smart lighting for roads allows lighting to be dynamically controlled and also adaptive to ambient conditions.

• Smart light connected to the Internet can be controlled remotely to configure lighting schedules and lighting intensity.

• Custom lighting configurations can be set for different situations such as a foggy day, a festival, etc.

**3.Smart Roads**

• Smart Roads provides information on driving conditions, travel time estimates and alerts in case of poor driving conditions, traffic congestions and accidents.

• Such information can help in making the roads safer and help in reducing traffic jams

• Information sensed from the roads can be communicated via internet to cloud-based applications and social media and disseminated to the drivers who subscribe to such applications.

**4.Structural Health Monitoring**

• It uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.

• The data collected from these sensors is analyzed to assess the health of the structures.

• By analyzing the data it is possible to detect cracks and mechanical breakdowns, locate the damages to a structure and also calculate the remaining life of the structure.

• Using such systems, advance warnings can be given in the case of imminent failure of the structure

**5.Surveillance**

• Surveillance of infrastructure, public transport and events in cities is required to ensure safety and security.

• City wide surveillance infrastructure comprising of large number of distributed and Internet connected video surveillance cameras can be created.

• The video feeds from surveillance cameras can be aggregated in cloud-based scalable storage solutions.

• Cloud-based video analytics applications can be developed to search for patterns of specific events from the video feeds.

**6.Emergency Response**

• IoT systems can be used for monitoring the critical infrastructure cities such as buildings, gas, and water pipelines, public transport and power substations.

• IoT systems for critical infrastructure monitoring enable aggregation and sharing of information collected from lager number of sensors.

• Using cloud-based architectures, multi-modal information such as sensor data, audio, video feeds can be analyzed I near real-time to detect adverse events.

• The alert can be in the form : Alerts sent to the public Re-rerouting of traffic Evacuations of the affected areas.

**Smart environments:**

1. Weather Monitoring
2. Air Pollution Monitoring
3. Noise Pollution Monitoring
4. Forest Fire Detection
5. River Flood Detection

**1.Weather Monitoring**

• It collects data from a number of sensor attached such as temperature, humidity, pressure, etc and send the data to cloud-based applications and store back-ends.

• The data collected in the cloud can then be analyzed and visualized by cloud-based applications.

• Weather alert can be sent to the subscribed users from such applications.

• AirPi is a weather and air quality monitoring kit capable of recording and uploading information about temperature, humidity, air pressure, light levels, UV levels, carbon monoxide, nitrogen dioxide and smoke level to the Internet.

**2.Air Pollution Monitoring**

• IoT based air pollution monitoring system can monitor emission of harmful gases by factories and automobiles using gaseous and meteorological sensors.

• The collected data can be analyzed to make informed decisions on pollutions control approaches.

**3.Noise Pollution Monitoring**

• Noise pollution monitoring can help in generating noise maps for cities.

• It can help the policy maker in making policies to control noise levels near residential areas, school and parks.

• It uses a number of noise monitoring stations that are deployed at different places in a city.

• The data on noise levels from the stations is collected on servers or in the cloud and then the collected data is aggregate to generate noise maps.

**4.Forest Fire Detection**

• IoT based forest fire detection system use a number of monitoring nodes deployed at different location in a forest.

• Each monitoring node collects measurements on ambient condition including temperature, humidity, light levels, etc.

• Early detection of forest fires can help in minimizing the damage.

**5.River Flood Detection**

• IoT based river flood monitoring system uses a number of sensor nodes that monitor the water level using ultrasonic sensors and flow rate using velocity sensors.

• Data from these sensors is aggregated in a server or in the cloud, monitoring applications raise alerts when rapid increase in water level and flow rate is detected.

**Smart energy systems:**

1. Smart Grid

2. Renewable Energy Systems

3. Prognostics

**1.Smart Grids**

• Smart grid technology provides predictive information and recommendation s to utilize, their suppliers, and their customers on how best to manage power.

• Smart grid collect the data regarding : - Electricity generation - Electricity consumption - Storage - Distribution and equipment health data

• By analyzing the data on power generation, transmission and consumption of smart grids can improve efficiency throughout the electric system.

• Storage collection and analysis of smarts grids data in the cloud can help in dynamic optimization of system operations, maintenance, and planning.

• Cloud-based monitoring of smart grids data can improve energy usage usage levels via energy feedback to users coupled with real-time pricing information.

• Condition monitoring data collected from power generation and transmission systems can help in detecting faults and predicting outages.

**2.Energy Renewable Energy System**

• Due to the variability in the output from renewable energy sources (such as solar and wind), integrating them into the grid can cause grid stability and reliability problems.

• IoT based systems integrated with the transformer at the point of interconnection measure the electrical variables and how much power is fed into the grid

• To ensure the grid stability, one solution is to simply cut off the overproductions.

**3.Energy Prognostics**

• IoT based prognostic real-time health management systems can predict performance of machines of energy systems by analyzing the extent of deviation of a system from its normal operating profiles.

• In the system such as power grids, real time information is collected using specialized electrical sensors called Phasor Measurement Units (PMU)

• Analyzing massive amounts of maintenance data collected from sensors in energy systems and equipment can provide predictions for impending failures.

• OpenPDC is a set of applications for processing of streaming time-series data collected from Phasor Measurements Units (PMUs) in real-time.

**Smart retail systems:**

1. Inventory Management

2. Smart Payments

3. Smart Vending Machines

**1.Retail Inventory Management**

• IoT system using Radio Frequency Identification (RFID) tags can help inventory management and maintaining the right inventory levels.

• RFID tags attached to the products allow them to be tracked in the real-time so that the inventory levels can be determined accurately and products which are low on stock can be replenished.

• Tracking can be done using RFID readers attached to the retail store shelves or in the warehouse

**2.Smart Payments**

• Smart payments solutions such as contact-less payments powered technologies such as Near field communication (NFC) and Bluetooth.

• NFC is a set of standards for smart-phones and other devices to communicate with each other by bringing them into proximity or by touching them

• Customer can store the credit card information in their NFC-enabled smart-phones and make payments by bringing the smart-phone near the point of sale terminals.

• NFC maybe used in combination with Bluetooth, where NFC initiates initial pairing of devices to establish a Bluetooth connection while the actual data transfer takes place over Bluetooth.

**3.Smart Vending Machines**

• Smart vending machines connected to the Internet allow remote monitoring of inventory levels, elastic pricing of products, promotions, and contact-less payments using NFC.

• Smart-phone applications that communicate with smart vending machines allow user preferences to be remembered and learned with time. E.g: when a user moves from one vending machine to the other and pair the smart-phone, the user preference and favourite product will be saved and then that data is used for predictive maintenance.

• Smart vending machines can have communicated each other's, so if a product out of stock in a machine, the user can be routed to nearest machine

• For perishable items, the smart vending machines can reduce the price as the expiry date nears.

**Smart logistic systems:**

1. Fleet Tracking

2. Shipment Monitoring

3. Remote Vehicle Diagnostics

**1.Logistics Fleet Tracking**

• Vehicle fleet tracking systems use GPS technology to track the locations of the vehicles in the real- time.

• Cloud-based fleet tracking systems can be scaled up on demand to handle large number of vehicles,

• The vehicle locations and routers data can be aggregated and analyzed for detecting bottlenecks I the supply chain such as traffic congestions on routes, assignments and generation of alternative routes, and supply chain optimization

**2.Logistics Shipment Monitoring**

• Shipment monitoring solutions for transportation systems allow monitoring the conditions inside containers.

• E.g : Containers carrying fresh food produce can be monitored to prevent spoilage of food. IoT based shipment monitoring systems use sensors such as temperature, pressure, humidity, for instance, to monitor the conditions inside the containers and send the data to the cloud, where it can be analyzed to detect food spoilage.

**3.Logistics Remote Vehicle Diagnostics**

• It can detect faults in the vehicles or warn of impending faults.

• These diagnostic systems use on-board IoT devices for collecting data on vehicle operation such as speed, engine RPM, coolent temperature, fault code number and status of various vehicle sub- system.

• Modern commercial vehicles support on-board diagnostic (OBD) standard such as OBD-II

• OBD systems provide real-time data on the status of vehicle sub-systems and diagnostic trouble codes which allow rapidly identifying the faults in the vehicle.

• IoT based vehicle diagnostic systems can send the vehicle data to centralized servers or the cloud where it can be analyzed to generate alerts and suggest remedial actions.

**Smart agriculture:**

1. Smart Irrigation

2. Green House Control

**1.Smart Irrigation**

• Smart irrigation system can improve crop yields while saving water.

• Smart irrigation systems use IoT devices with soil moisture sensors to determined the amount of moisture on the soil and release the flow of the water through the irrigation pipes only when the moisture levels go below a predefined threshold.

• It also collect moisture level measurements on the server on in the cloud where the collected data can be analyzed to plan watering schedules.

- Cultivar’s RainCould is a device for smart irrigation that uses water valves, soil sensors, and a WiFi enabled programmable computer

**2.Green House Control**

- It controls temperature, humidity, soil, moisture, light, and carbon dioxide level that are monitored by sensors and climatological conditions that are controlled automatically using actuation devices.

- IoT systems play an importance role in green house control and help in improving productivity.
- The data collected from various sensors is stored on centralized servers or in the cloud where analysis is performed to optimize the control strategies and also correlate the productivity with different control strategies.

**Smart industry:**

1. Machine Diagnosis & Prognosis

2. Indoor Air Quality Monitoring

**1.Machine Diagnosis & Prognosis**

- Machine prognosis refers to predicting the performance of machine by analyzing the data on the current operating conditions and how much deviations exist from the normal operating condition.

- Machine diagnosis refers to determining the cause of a machine fault.

- Sensors in machine can monitor the operating conditions such as temperature and vibration levels, sensor data measurements are done on timescales of few milliseconds to few seconds which leads to generation of massive amount of data.

- Case-based reasoning (CBR) is a commonly used method that finds solutions to new problems based on past experience.

- CBR is an effective technique for problem solving in the fields in which it is hard to establish a quantitative mathematical model, such as machine diagnosis and prognosis.

**2.Indoor Air Quality Monitoring**

- Harmful and toxic gases such as carbon monoxide (CO), nitrogen monoxide (NO), Nitrogen Dioxide, etc can cause serious health problem of the workers.

- IoT based gas monitoring systems can help in monitoring the indoor air quality using various gas sensors. - The indoor air quality can be placed for different locations

- Wireless sensor networks based IoT devices can identify the hazardous zones, so that corrective measures can be taken to ensure proper ventilation.

**Smart health & lifestyle:**

1.Health & Fitness Monitoring

2. Wearable Electronics

**1.Health & Fitness Monitoring**

• Wearable IoT devices allow to continuous monitoring of physiological parameters such as blood pressure, heart rate, body temperature, etc than can help in continuous health and fitness monitoring.

• It can analyze the collected health-care data to determine any health conditions or anomalies.

• The wearable devices may can be in various form such as: • Belts • Wrist-bands

**2.Health & Lifestyle Wearable Electronics**

• Wearable electronics such as wearable gadgets (smart watch, smart glasses, wristbands, etc) provide various functions and features to assist us in our daily activities and making us lead healthy lifestyles.

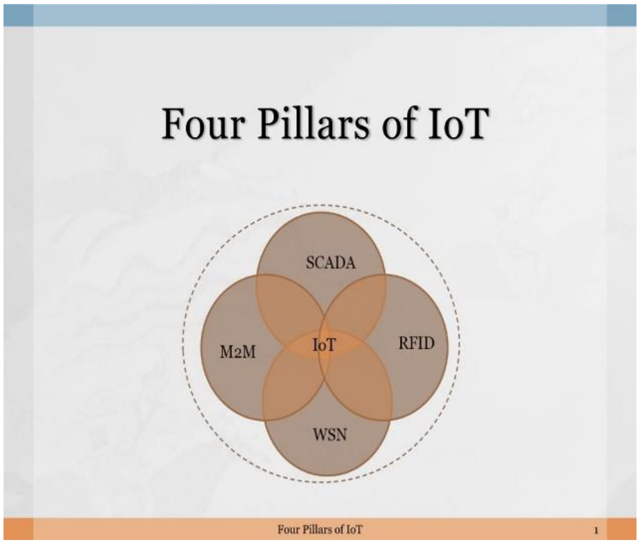
• Using the smart watch, the users can search the internet, play audio/video files, make calls, play games, etc.

• Smart glasses allows users to tae photos and record videos, get map directions, check flight status or search internet using voice commands

• Smart shoes can monitor the walking or running speeds and jumps with the help of embedded sensors and be paired with smart-phone to visualize the data.

• Smart wristbands can tract the daily exercise and calories burnt.

**Four Pillars of IoT**



Four Pillars of IoT

Four Pillars of IoT 1

## A four-pillar graphic is introduced for the broader IoT

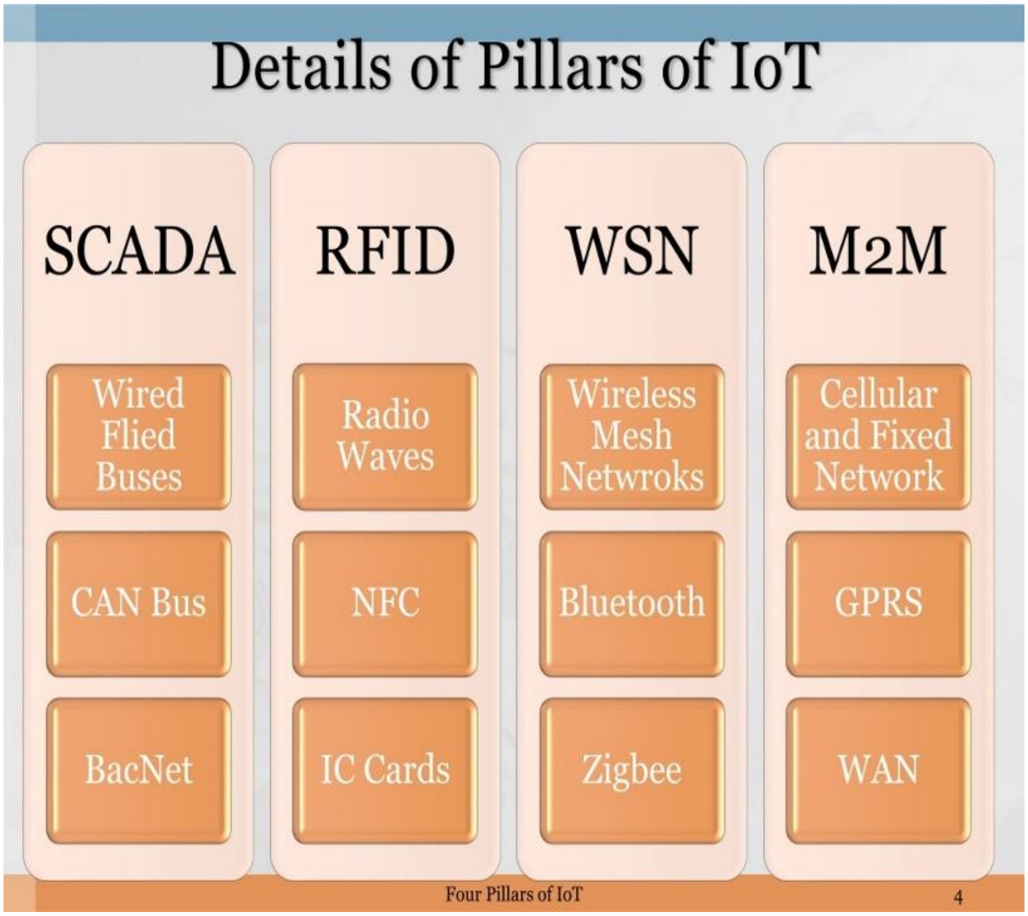
The four pillars of IoT are • M2M • RFID • WSNs • SCADA (supervisory control and data acquisition)

• M2M uses devices to capture events, via a network connection to a central server, that translates the captured events into meaningful information.

• RFID uses radio waves to transfer data from an electronic tag attached to an object to a central system through a reader for the purpose of identifying and tracking the object.

• A WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions.

• SCADA is an autonomous system based on closed-loop control theory or a smart system or a CPS data connects, monitors, and controls equipment via network in a facility such as a plant or a building. Four Pillars of IoT



Details of Pillars of IoT

| SCADA | RFID | WSN | M2M |
|---|---|---|---|
| Wired Flied Buses | Radio Waves | Wireless Mesh Netwroks | Cellular and Fixed Network |
| CAN Bus | NFC | Bluetooth | GPRS |
| BacNet | IC Cards | Zigbee | WAN |

Four Pillars of IoT 4

**1. M2M: The Internet of Devices** • Machine to machine refers to direct communication between devices using any communications channel, including wired and wireless. Machine to machine communication can include industrial instrumentation, enabling a sensor or meter to communicate the data it records (such as temperature, inventory level, etc.) to application software that can use it. • Most of the M2M market research reports assume M2M modules are simply just cellular modules. Four Pillars of IoT

**Application Areas for Cellular M2M, p. 67** • There is overlap between M2M and the consumer electronics applications. The consumer electronics offerings include the following: • Personal navigation devices • eReaders • Digital picture frames • People-tracking devices • Pet-tracking devices • Home security monitors • Personal medical devices Four Pillars of IoT

**The typical architecture of an M2M system from BiTX.** • Service S N 7 Asset-specific protocol 6 M2M communication protocol N S Network adapter Gateway Manager Four Pillars of IoT

2. **RFID: The Internet of Objects** • An RFID tag is a simplified, low-cost, disposable contactless smartcard. RFID tags include a chip that stores a static number (ID) and attributes of the tagged object and an antenna that enables the chip to transmit the store number to a reader. • An RFID system involves hardware known as readers and tags, as well as RFID software or RFID middleware.

**3. WSN: The Internet of Transducers** • WSN is more for sensing and information-collecting purposes. Other networks include body sensor network (BSN), visual or video sensor network (VSN), vehicular sensor networks, underwater (acoustic) sensor networks, interplanetary sensor networks, fieldbus networks, and others. • The extended scope of WSN is the USN, or ubiquitous sensor network, a network of intelligent sensors that could one day become ubiquitous.

**The architecture of a typical sensor network** • Sensor node: sense target events, gather sensor readings, manipulate information, send them to gateway via radio link • Base station/sink: communicate with sensor nodes and user/operator • Operator/user: task manager, send query • Routing and energy saving are required. Four Pillars of IoT

**WSNs are meant to be deployed in large numbers in various** environments, including remote and hostile regions, with ad hoc communications as key. • For this reasons, algorithms and protocols need to address the following issues. • Lifetime maximization • Robustness and fault tolerance • Self-configuration • Middleware for WSN, the middle-level primitive between the software and the hardware, can help bridge the gap and remove impediments. Four Pillars of IoT

**Context-aware system based on WSN** • Mobile sensor networks (MSNs) are WSNs in which nodes can move under own control or under the control of the environment. Four Pillars of IoT

**4. SCADA: The Internet of Controllers** • SCADA (supervisory control and data acquisition) is a type of industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world • An existing SCADA system usually consists of the following subsystems: • HMI (human-machine interface) • RTU (remote terminal units) • PLCs (programmable logic controllers) • DCSs (distributed control systems) • M2M, WSN, smart systems, CPS, and others all have overlaps of scope with SCADA. Four Pillars of IoT